Symantec™ Event Collector for Network Associates® ePO and VirusScan® Integration Guide

Symantec™ Event Collector for Network Associates® ePO and VirusScan® Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.1

Copyright Notice

Copyright © 2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. SESA, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation.

IBM is a trademark of the IBM Corporation.

McAfee, VirusScan, and Network Associates are registered trademarks of Network Associates and/or its affiliates in the U.S. and/or other countries.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
COLLECTORS

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompany this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use each licensed copy of the Software on a single central processing unit; and

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software to collect data from a type of technology other than when using a Symantec Event Manager product that corresponds to that type of technology (i.e., antivirus, firewall, IDS, etc.); nor

G. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which You have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Technical support

Chapter 1 Introducing Symantec Event Collector for Network Associates ePO and VirusScan

About Symantec Event Collector for Network Associates ePO and VirusScan 10
About installation 11
About SESA integration component installation 12
About Event Collector installation 12
Symantec Event Collector for Network Associates ePO and VirusScan CD contents 13

Chapter 2 Installing Symantec Event Collector for Network Associates ePO and VirusScan

Before installing Symantec Event Collector for Network Associates ePO and VirusScan 16
Planning the Event Collector setup 16
Suggested Event Collector installation configurations 17
Network Associates VirusScan configuration considerations 19
Language considerations 20
System requirements 22
Network Associates product support 22
Event Collector system requirements 22
Installing Symantec Event Collector for Network Associates ePO and VirusScan 23
Installing SESA integration components using the SESA Integration Wizard 24
Installing the Event Collector 27
Installing the Event Collector silently 31
Changing the access rights of the Symantec Collector Framework service 35
Adding other product Plug-ins to the Event Collector 36
Configuring the ePO Event Collector for languages other than English 37
Verifying the installation 38

Starting and stopping services 40
Troubleshooting the Symantec Event Collector for Network Associates ePO and VirusScan installation 41
Verifying SESA integration component installation 41
Verifying Event Collector operation 42
Troubleshooting the Network Associates ePolicy Orchestrator Plug-in 43
Troubleshooting the Network Associates VirusScan Plug-in 44
Uninstalling Symantec Event Collector for Network Associates ePO and VirusScan 44
Uninstalling the Event Collector 44
Uninstalling the SESA integration components 46

Appendix A Event Collector configuration file options

Collector.cfg file configuration options 50
MVSSesa.cfg file configuration options 51
EPOSesa.cfg file configuration options 53

Appendix B Command-line options

Installing Symantec Event Collector for Network Associates ePO and VirusScan components manually 56
Installing the SESA Agent 56
Uninstalling the SESA Agent 58
Guidelines for using scripts to install the Event Collector 59
Event Collector installation scripts 60
Event Collector uninstallation scripts 61
Plug-in installation and uninstallation scripts 62
Plug-in load and unload scripts 62
Event Collector command-line options 62
SESA Integration Wizard command-line options 64

Index

Chapter 1

Introducing Symantec Event Collector for Network Associates ePO and VirusScan

This chapter includes the following topics:

- About Symantec Event Collector for Network Associates ePO and VirusScan
- About installation
- Symantec Event Collector for Network Associates ePO and VirusScan CD contents

About Symantec Event Collector for Network Associates ePO and VirusScan

Symantec Event Collector for Network Associates ePO and VirusScan enables centralized, cross-tier logging, alerting, and reporting between the Symantec Enterprise Security Architecture (SESA) event management system and Network Associates VirusScan.

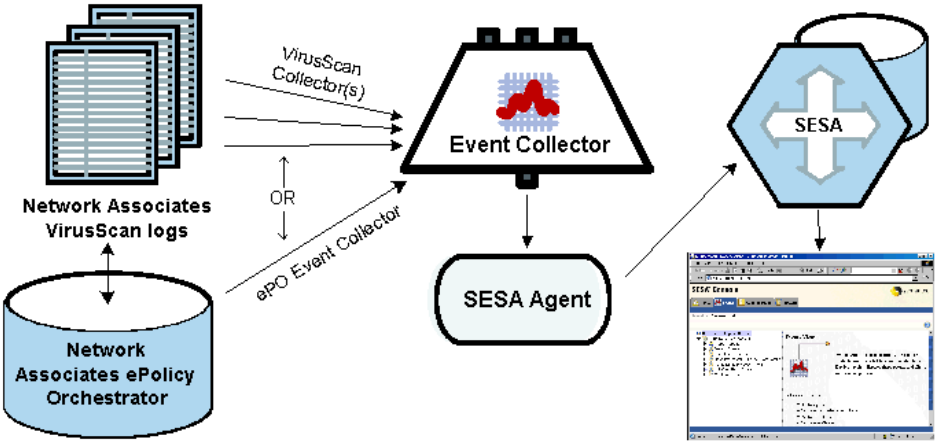
Depending on whether you are using Network Associates ePolicy Orchestrator (ePO) to retrieve VirusScan events or are using VirusScan logs to retrieve events, you use Symantec Event Collector for Network Associates ePO and VirusScan to install the following:

- ePO Event Collector: Collects VirusScan events from the ePO database.
- VirusScan Event Collector: Collects VirusScan events from VirusScan logs.

Once you install Symantec Event Collector for Network Associates ePO and VirusScan, Network Associates VirusScan will be SESA-enabled. When a product is SESA-enabled, you can use the SESA Console to view the events that it forwards to SESA. The SESA Console provides a central location in which to view and manage the reporting of event data across multiple SESA-enabled security products.

Figure 1-1 shows how VirusScan events are collected by the Event Collector and sent to SESA.

Figure 1-1 How the Event Collector collects and sends events to SESA



SESA is an event management system that employs data collection services for events that Symantec security products generate. For more information on SESA, see the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator's Guide*.

About installation

Symantec Event Collector for Network Associates ePO and VirusScan installs shared and product-specific components to enable Network Associates VirusScan event logs or Network Associates ePolicy Orchestrator to send VirusScan events to SESA.

To enable Network Associates VirusScan logs or ePO to forward events to SESA, Symantec Event Collector for Network Associates ePO and VirusScan installs the following components:

SESA integration components on the SESA Manager computer	The integration components extend SESA functionality to use the Event Collector and include support for VirusScan event data.
An Event Collector and SESA Agent on the same computer	An Event Collector is comprised of an Event Collector Framework and a Network Associates VirusScan Plug-in or Network Associates ePolicy Orchestrator Plug-in, as required by your VirusScan installation.

The Event Collector Framework is a technology into which the Plug-ins of supported products are installed. Together, the Framework and the appropriate Plug-in collect event data from their VirusScan data sources and forward it to SESA. The Collector Framework architecture manages the loading and registration of the Plug-ins, and forwards messages related to itself and the administration of the Plug-ins. The Framework does not forward existing events from Network Associates VirusScan or ePolicy Orchestrator. It only reports events that relate to the success or failure of itself or the Plug-ins.

Plug-ins are responsible for forwarding already existing events that have been generated by their respective VirusScan products. As such, the Plug-ins act as a proxy for their products. They do not create their own events.

You install the SESA integration components and the Event Collector in separate procedures.

About SESA integration component installation

The first phase of installing Symantec Event Collector for Network Associates ePO and VirusScan is to extend SESA functionality to use the Event Collector and VirusScan event data.

To enable SESA support, you install the SESA integration components for Network Associates VirusScan and the Event Collector Framework on the computer on which the SESA Manager is installed. You install the components by running two SESA Integration Wizards on the SESA Manager computer. You run one SESA Integration Wizard to extend SESA functionality to use the Event Collector. You run another SESA Integration Wizard to extend SESA functionality to include VirusScan event data.

The extended functionality lets you centrally view and manage reports for VirusScan events in the SESA Console.

About Event Collector installation

The second phase of installing Symantec Event Collector for Network Associates ePO and VirusScan is to install the appropriate Event Collector. The Event Collector collects events from the VirusScan logs or ePO database, formats them, and sends them to the SESA Agent. The SESA Agent, which installs with the Event Collector, enables communication and configuration of events between SESA and the Network Associates product.

To install an ePO Event Collector or a VirusScan Event Collector, you use the Symantec Event Collector Installation Wizard.

Note: You install either the ePO Event Collector or the VirusScan Event Collector. If you install both Event Collectors, then VirusScan events are logged to SESA twice.

As a best practice, you install the Event Collector on the same computer that is running Network Associates VirusScan. The ePO database can reside on a separate computer.

Which Event Collector you install depends on how Network Associates VirusScan is operating in your environment.

See "Suggested Event Collector installation configurations" on page 17.

Symantec Event Collector for Network Associates ePO and VirusScan CD contents

The Symantec Event Collector for Network Associates ePO and VirusScan CD contains folders for each of its supported products as well as for the Event Collector.

Symantec Event Collector for Network Associates ePO and VirusScan CD folders, their contents, and subdirectories are listed in Table 1-1.

Table 1-1 Symantec Event Collector for Network Associates ePO and VirusScan CD contents

CD folder	Contents
\Acrobat	Adobe Acrobat Reader 5.05
\Collector	■ Event Collector component files, which include the Collector Framework and the Network Associates VirusScan and Network Associates ePO Plug-ins ■ Event Collector Installation Wizard that is used to install the Event Collector components ■ Event Collector configuration files
\Collector\SESA	■ SESA Agent installation files ■ SESA Integration Wizard ■ SESA integration components for the Collector Framework
\Docs	■ Readme.txt ■ SEC_NA.PDF (*Symantec Event Collector for Network Associates ePO and VirusScan Integration Guide*)
\VirusScan\SESA	■ SESA Integration Wizard ■ SESA integration components for Network Associates VirusScan

Chapter 2

Installing Symantec Event Collector for Network Associates ePO and VirusScan

This chapter includes the following topics:

- Before installing Symantec Event Collector for Network Associates ePO and VirusScan
- Planning the Event Collector setup
- System requirements
- Installing Symantec Event Collector for Network Associates ePO and VirusScan
- Verifying the installation
- Starting and stopping services
- Troubleshooting the Symantec Event Collector for Network Associates ePO and VirusScan installation
- Uninstalling Symantec Event Collector for Network Associates ePO and VirusScan

Before installing Symantec Event Collector for Network Associates ePO and VirusScan

Before you install Symantec Event Collector for Network Associates ePO and VirusScan, make sure that the following conditions have been met:

SESA	Make sure that SESA is installed and operating properly. For more information, see the *Symantec Enterprise Security Architecture Installation Guide*.
Network Associates products	Make sure that Network Associates VirusScan 4.51 or 4.51 with Service Pack 1 is installed and operating properly. If in use, make sure that ePolicy Orchestrator Server 2.5.0 and the supported ePO database are installed and operating properly. For more information, see your Network Associates product documentation.
Event Collector setup	Make sure that you install the appropriate Event Collector based on your Network Associates VirusScan installation. In addition, make sure that you have optimally configured Network Associates VirusScan to operate as a SESA-enabled product. If your VirusScan product is in a language other than English, you must configure the Event Collector accordingly. See "Planning the Event Collector setup" on page 16.
Java Runtime Environment (JRE)	Make sure that the computer on which you install the SESA Agent is running Java Runtime Environment (JRE) or is hosting the SESA Manager. JRE versions 1.2.2_008 through 1.3.1_02 are supported. JRE version 1.3.1_02 is provided on the SESA CD1 - SESA Manager in the \Utils\JRE folder. Double-click j2re-1_3_1_02-win-i.exe, then follow the on-screen instructions.

Planning the Event Collector setup

For Network Associates VirusScan to operate successfully and efficiently as a SESA-enabled product, you must plan accordingly for how your VirusScan or ePO Event Collector will operate in your SESA and Network Associates environment.

Suggested Event Collector installation configurations

Depending on how Network Associates VirusScan is running in your network environment, you will install the VirusScan Event Collector or the ePO Event Collector.

Table 2-1 contains suggested Event Collector installation configurations based on the way that you have installed Network Associates VirusScan across your network environment.

Table 2-1 Suggested Event Collector installation configurations

Network Associates environment	Suggested Event Collector installation configuration
Network Associates VirusScan is installed and using the ePO database to store event data.	Install a single ePO Event Collector to collect VirusScan events from ePO. To manage all VirusScan computers that are managed by ePO, install one ePO Event Collector on each ePO Server.
ePO is not handling VirusScan events.	Install the VirusScan Event Collector on each VirusScan client computer. This method of VirusScan Event Collector installation configuration is recommended. See "Benefits of installing the VirusScan Event Collector on each VirusScan client computer" on page 18.
You have Windows 9x VirusScan client computers.	Install the VirusScan Event Collector on a Windows 2000 or Windows XP computer or computers. See "Event Collector system requirements" on page 22. Because the Event Collector does not install on Windows 9x computers, you must ensure that the Windows 2000/XP computers have network read access to the VirusScan logs on the Windows 9x computers. On Windows 9x computers, ensure that you also create a file share for the log folder.

If you choose to install the VirusScan Event Collector, you select the Network Associates VirusScan Plug-in when you run the Event Collector Installation Wizard. After the VirusScan Plug-in is installed and registered with the Event Collector Framework, it queries existing VirusScan logs (at a polling cycle that you set during installation) and forwards the messages to the SESA Manager.

If you choose to install the ePO Event Collector, you select the Network Associates ePolicy Orchestrator Plug-in when you run the Event Collector Installation Wizard. After the Network Associates ePO Plug-in is installed and registered with the Event Collector Framework, it queries the ePO database and forwards the VirusScan events to the SESA Manager.

You can also configure the installation of the Event Collector by executing Event Collector command-line options.

See "Event Collector command-line options" on page 62.

Benefits of installing the VirusScan Event Collector on each VirusScan client computer

When you do not have ePO installed to handle Network Associates VirusScan events, the best way to install the VirusScan Event Collector is on each VirusScan client computer.

Installing the Event Collector on each client computer results in the following benefits:

- Event Collector setup and configuration are easier because you can avoid having to create network file shares on each VirusScan client computer.
- Less network traffic is involved in polling network shares and reading event information from VirusScan log files.
- The version of Network Associates VirusScan is reported correctly. When the VirusScan Event Collector reads data across network file shares, version information is not reported.
- The latent period in reporting events from a particular VirusScan client computer is decreased (for example, a computer at the end of a list of network file shares).

Network Associates VirusScan configuration considerations

To ensure that Network Associates VirusScan integrates successfully with SESA, follow the best practices contained in Table 2-2 when you use VirusScan as a SESA-enabled product.

Table 2-2 Network Associates VirusScan best practices

VirusScan vulnerability	Best practice
VirusScan logging to local drives	Ensure that you install the VirusScan Event Collector on each VirusScan client computer, because VirusScan client computers can only log to local hard drives and not to shared network volumes. If you cannot install to each VirusScan client computer, then create a network share on each VirusScan client computer, and then install a single Event Collector on another computer that can collect each shared log folder.
Log file reporting	Configure log file reporting in Network Associates VirusScan to log all information for all scan tasks. If space is a concern, you can disable the logging of Session settings and Session summary. When you disable any other log information, the ability of the Event Collector to successfully collect all events is diminished.
Log file size	Avoid log file size limits for scans. If you configure VirusScan to limit log file size, then the Event Collector cannot collect the new events it receives after the log file has reached its maximum size.

Table 2-2 Network Associates VirusScan best practices

VirusScan vulnerability	Best practice
Log file paths and event collection	Configure the VirusScan Event Collector to collect events from scheduled scans as well as VirusShield (auto-protect), manual, and new scheduled scans. The default VirusScan log path for scheduled scans is not the same one as the two scheduled scans (Scan My Computer and Scan Drive 'C') that are provided at installation. By default, VirusShield, manual, and new scheduled scans log events to the following standard location: C:\Program Files\Network Associates\VirusScan However, the two scheduled scans log events to the following location: C:\Program Files\Common Files\Network Associates\On Demand Scanner\Scan32 To collect events from all scans, you must modify the log path locations to match or modify the PluginLogPath*n* and PluginLogPathCount options in the MVSSesa.cfg file to include both log paths. See "MVSSesa.cfg file configuration options" on page 51.
Log file deletion or truncation	Be aware of how the Event Collector treats log files that have been truncated or deleted after the Event Collector has read the last entry. If the log file is deleted or truncated since the last entry was read, then the Event Collector will not be able to collect more events from the log file.

For more information, see your Network Associates VirusScan product documentation.

Language considerations

When Network Associates products or Event Collectors are in a language other than English, you will need to plan your installation environment accordingly.

ePO Event Collector language considerations

The ePO Event Collector supports event and action descriptions for the languages in Table 2-3.

Table 2-3 ePO Event Collector supported languages

Language	ID
French	040C
German	0407
Spanish	040A
English	0409
Japanese	0411

To report VirusScan events to SESA in a language other than English, you must specify the appropriate language ID in the ePolicy Orchestrator Plug-in (ePOSesa.cfg) configuration file. In addition, you modify the CollectorLocale option to include the appropriate language in the Collector.cfg file.

See "EPOSesa.cfg file configuration options" on page 53.

See "Collector.cfg file configuration options" on page 50.

If you are configuring the ePO Event Collector to report VirusScan events in a language other than English, make sure that the ePO Event Collector is installed on an operating system in the same language as the reported VirusScan events. Matching the VirusScan event language and the ePO Event Collector operating system language ensures that translation is performed using the correct character set. This is especially important for Japanese.

As a best practice, make sure that Network Associates ePolicy Orchestrator is also installed on a computer with an operating system in the appropriate language. Again, this is especially important for Japanese.

VirusScan Event Collector language considerations

If you are using an English version of the VirusScan Event Collector, be aware that it can only collect VirusScan events from English version VirusScan logs that are generated by English version VirusScan products.

If you are using a VirusScan Event Collector in a language other than English, you must install the VirusScan Event Collector on a computer that has an operating system in the same language as the VirusScan logs and the VirusScan Event Collector.

When the VirusScan Event Collector is in a language other than English, it can only collect VirusScan log data in the same language.

System requirements

Before you install Symantec Event Collector for Network Associates ePO and VirusScan, make sure that the computer or computers on which you will install the Event Collector meet the necessary requirements. In addition, the computer on which the SESA DataStore is installed must have enough hard disk space to accommodate the additional security events that the Network Associates VirusScan logs or Network Associates ePO database will send to it.

Network Associates product support

Symantec Event Collector for Network Associates ePO and VirusScan supports the following Network Associates products:

- Network Associates VirusScan 4.5.1 and 4.5.1 with Service Pack 1
- Network Associates ePolicy Orchestrator Server 2.5.0
- Network Associates ePolicy databases: MSDE (installed with ePO), MS SQL Server 7 with Service Pack 3, and MS SQL Server 2000

Event Collector system requirements

Symantec Event Collector for Network Associates ePO and VirusScan installs the SESA Agent and the Event Collector on the same computer. The computer on which you install the SESA Agent must meet the following minimum system requirements:

Operating system	■ Windows 2000 Server with Service Pack 2 ■ Windows 2000 Advanced Server with Service Pack 2 ■ Windows 2000 Professional with Service Pack 2 ■ Windows XP Professional
SESA version	This version of Symantec Event Collector for Network Associates ePO and VirusScan requires SESA version 1.1.
Sun Java requirements	Java Runtime Environment (JRE) versions 1.2.2_008 through 1.3.1_02 JRE is not required if the Event Collector is installed on the SESA Manager computer.

Processor	Intel Pentium-compatible 133-MHz processor
Memory	■ 32 MB of memory for the SESA Agent ■ 64 MB RAM for each Symantec security product (128 MB or more recommended)
Hard disk space	■ 26 MB of hard disk space for Event Collector Framework program files ■ 300 KB of hard disk space for the Network Associates VirusScan Plug-in or the Network Associates ePolicy Orchestrator Plug-in program files
Network connection	TCP/IP connection to network

The RunAsService service must be set to manual startup, set to automatic startup, or running during the Event Collector installation. You can disable the service after installation, if desired.

Installing Symantec Event Collector for Network Associates ePO and VirusScan

To enable Network Associates VirusScan or ePolicy Orchestrator to send events to SESA, you install Symantec Event Collector for Network Associates ePO and VirusScan in the phases described in Table 2-4.

Table 2-4 Phased installation

Installation location	Installation phase
On each SESA Manager computer to which Network Associates VirusScan events are forwarded	Run two SESA Integration Wizards: one for the Event Collector Framework and the other for the VirusScan product that you installed. The wizard installs the appropriate SESA integration components for the Event Collector Framework and the VirusScan product. See "Installing SESA integration components using the SESA Integration Wizard" on page 24.

Table 2-4 Phased installation

Installation location	Installation phase
On one or more computers that read VirusScan log files or the ePO database	Install the Event Collector Framework and necessary Plug-ins using the Symantec Event Collector Installation Wizard. If Network Associates ePolicy Orchestrator is handling the VirusScan logs, then install the Network Associates ePolicy Orchestrator Plug-in. If you want the Event Collector to collect events directly from the Network Associates VirusScan logs, then install the Network Associates VirusScan Plug-in. See "Installing the Event Collector" on page 27.

You first use the SESA Integration Wizard to extend SESA functionality to support the Event Collector and the Network Associates product that you are enabling to forward events to SESA.

After you extend SESA functionality to support your product, you install the appropriate Event Collector using the Symantec Event Collector Installation Wizard.

Installing SESA integration components using the SESA Integration Wizard

You must run the SESA Integration Wizard on each SESA Manager computer for the Event Collector Framework. You must also run the SESA Integration Wizard for Network Associates VirusScan. The SESA Integration Wizard installs the appropriate SESA integration components for the Event Collector and Network Associates VirusScan, and extends SESA functionality to support both.

Install SESA integration components using the SESA Integration Wizard

To enable the Network Associates product to send events to SESA, you must run the SESA Integration Wizard for the following:

- Event Collector Framework
  See "To install SESA integration components for the Event Collector Framework" on page 25.
- Network Associates VirusScan
  See "To install SESA integration components for Network Associates VirusScan" on page 26.

To install SESA integration components for the Event Collector Framework

1. On the computer on which the SESA Manager is installed, insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.
2. At the command prompt, change directories on the CD to \Collector\SESA.
3. At the command prompt, type **java -jar setup.jar**
   The SESA Integration Wizard starts.
4. Follow the on-screen instructions until you see the SESA Domain Administrator Information window.

5 In the SESA Domain Administrator Information window, do the following:

SESA Domain Administrator Name	Type the name of the SESA Domain Administrator account.
SESA Domain Administrator Password	Type the password for the SESA Domain Administrator account.
Host Name or IP Address of SESA Directory	Type one of the following: ■ If SESA is using default, anonymous SSL communications, the IP address of the computer on which the SESA Directory is installed (it may be the same as the SESA Manager IP address if they are both installed on the same computer). ■ If SESA is using authenticated SSL communication, the host name of the SESA Directory computer. For example, mycomputer.com. For more information on the SESA default, anonymous SSL, and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
Secure Directory Port	Type the number of the SESA Directory SSL (LDAP) port (by default, 636).

6 Follow the on-screen instructions to install the SESA integration components and complete the SESA Integration Wizard.

7 Repeat steps 1 through 6 on each SESA Manager computer to which you are forwarding Network Associates VirusScan events.

To install SESA integration components for Network Associates VirusScan

1 On the computer on which the SESA Manager is installed, insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.

2 At the command prompt, change directories on the CD to \VirusScan\SESA.

3 At the command prompt, type **java -jar setup.jar**
The SESA Integration Wizard starts.

4 Follow the on-screen instructions until you see the SESA Domain Administrator Information window.

5 In the SESA Domain Administrator Information window, do the following:

SESA Domain Administrator Name	Type the name of the SESA Domain Administrator account.
SESA Domain Administrator Password	Type the password for the SESA Domain Administrator account.
Host Name or IP Address of SESA Directory	Type one of the following: ■ If SESA is using default, anonymous SSL communications, the IP address of the computer on which the SESA Directory is installed (it may be the same as the SESA Manager IP address if they are both installed on the same computer). ■ If SESA is using authenticated SSL communication, the host name of the SESA Directory computer. For example, mycomputer.com. For more information on the SESA default, anonymous SSL, and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
Secure Directory Port	Type the number of the SESA Directory SSL (LDAP) port (by default, 636).

6 Follow the on-screen instructions to install the SESA integration components and complete the SESA Integration Wizard.

7 Repeat steps 1 through 6 on each SESA Manager computer to which you are forwarding Network Associates VirusScan events.

Installing the Event Collector

Symantec Event Collector for Network Associates ePO and VirusScan installs the Event Collector as a service with local system access rights. If you plan to use Integrated Windows Authentication to handle communication between the Event Collector and the ePO database, you must change the access rights of the Symantec Collector Framework service to at least query access to the ePO database after Event Collector installation.

In addition, if the Event Collector is configured to collect events from Network Associates VirusScan logs that reside on remote network shares, you must also

change the access rights of the Symantec Collector Framework service to have at least read-only access rights on the computer file shares on which the logs reside.

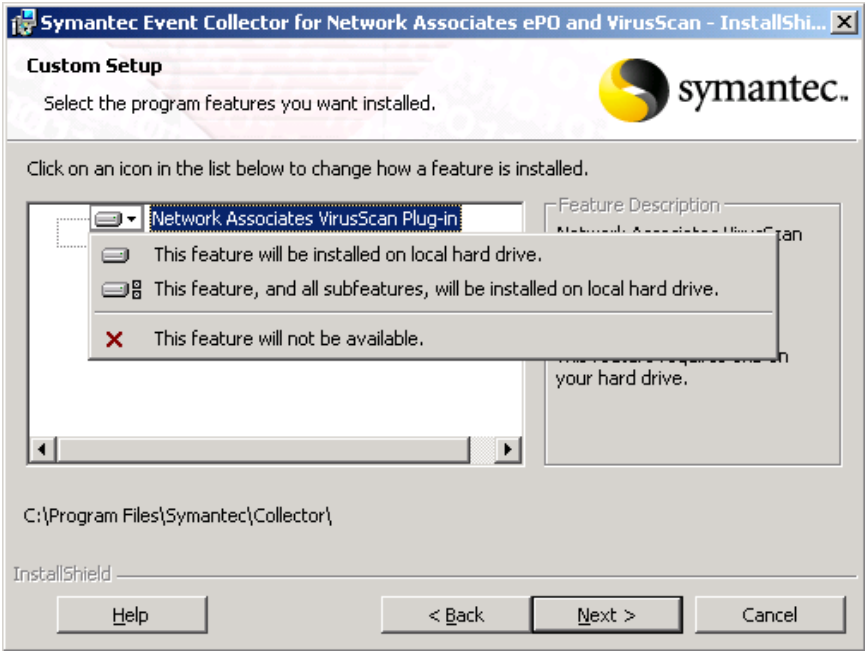
See "Changing the access rights of the Symantec Collector Framework service" on page 35.

See "Suggested Event Collector installation configurations" on page 17.

The RunAsService service must be set to manual startup, set to automatic startup, or running during the Event Collector installation. You can disable the service after installation, if desired.

To install the Event Collector

1. Insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.
2. Click **Next**, review and accept the license agreement, then click **Next** until you see the Custom Setup window.
3. In the Custom Setup window, next to the Network Associates Plug-in that you do not want to install, click the icon to display the Plug-in installation options.


Symantec Event Collector for Network Associates ePO and VirusScan - InstallShi...
Custom Setup
Select the program features you want installed.
symantec.
Click on an icon in the list below to change how a feature is installed.
Network Associates VirusScan Plug-in
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
Feature Description
your hard drive.
C:\Program Files\Symantec\Collector\
InstallShield
Help
< Back
Next >
Cancel

4 Click **This feature will not be available**.

By default, the Installation Wizard installs the Event Collector Framework and the Network Associates Plug-in that you are installing to C:\Program Files\Symantec\Collector.

5 To view the hard disk space requirements for the Network Associates Plug-in, make sure that the Network Associates Plug-in that you want is selected, then click **Space**.

6 Do one of the following:

- To change the default installation location of the Network Associates Plug-in, click **Change**, then in the Change Current Destination Folder window, click the appropriate Browse button to navigate to the new location. When the desired path for the new location is displayed under Folder name, click **OK**.

  You can also type the installation path as necessary.
- To accept the installation location, click **Next**.

7 In the Collector Configuration window, do one of the following:

- To change the default installation location of the vent Collect log file, click **Change**, then in the Change Current Destination Folder window, click the appropriate Browse button to navigate to the new location. When the desired path for the new location is displayed under Folder name, click **OK**.
- To accept the default Event Collector log location, click **Next**.

8 In the SESA Agent Configuration window, next to SESA Manager IP Address, do one of the following:

- If SESA is using default, anonymous SSL communications, type the IP address of the SESA Manager computer.
- If SESA has been configured to use authenticated SSL, type the host name of the SESA Manager computer.

  For example, mycomputer.com.

For more information on default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.

9 In the SESA Manager port number box, type the number of the SESA Manager secure port.

By default, the secure port number is 443.

10 Do one of the following:

- To change the default installation location of the SESA Agent, click **Change**, then in the Change Current Destination Folder window, click the appropriate Browse button to navigate to the new location. When the desired path for the new location is displayed under Folder name, click **OK**.
- To accept the default location, click **Next**.

  The default location is C:\Program Files\Symantec\SESA\Agent.

11 Do one of the following:

- In the Network Associates VirusScan Plug-in Configuration window, change the default polling frequency of the Network Associates VirusScan Plug-in if necessary.
- In the Network Associates ePO Plug-in Configuration window, change the default polling frequency of the Network Associates ePolicy Orchestrator Plug-in if necessary.

The polling frequency is the interval in seconds in which the Plug-in queries the VirusScan log files or ePO database for new data. The default polling frequency is five seconds.

12 Under How do you want to handle existing events?, select one of the following:

- Forward existing and new events: Forwards all existing events as well as new events
- Forward only new events (generated after this installation): Forwards only events that have been generated after the installation of the Event Collector

13 If Network Associates VirusScan is installed to a nondefault directory, or if the VirusScan logs are being collected remotely over network file shares, in the Network Associates VirusScan Plug-in Configuration window, click **Browse** to navigate to a new location for the log file, then click **OK**.

Alternatively, you can type a UNC path.

14 If you are installing the Network Associates ePolicy Orchestrator Plug-in, in the ePO Plug-In Configuration window, do one of the following:

- Click **Use Windows Integrated Authentication**, then in the Management Server and Database Server boxes, type the computer name of the ePO Management Server and Database Server respectively.

  You must change the service credentials of the Symantec Collector Framework service after installation.

  See "Changing the access rights of the Symantec Collector Framework service" on page 35.

- Click **Use SQL Server Authentication**, then type the name of the ePO Management Server and Database Server, and the SQL Username and SQL password.

  If the ePolicy Orchestrator installation is using an MSDE database, the the default SQL Username is sa with a blank (empty) password.

15 Follow the on-screen instructions to install the Event Collector and complete the Installation Wizard.

Installing the Event Collector silently

You can install the Event Collector and the SESA Agent by command line, rather than displaying the Event Collector Installation Wizard screens. This process is called a silent installation.

Install the Event Collector silently

To perform a silent installation of the Event Collector, you complete the following tasks:

- Modify the necessary configuration files: The information that you normally specify in the Event Collector Installation Wizard windows must be specified in the Agent.settings, MVSSesa.cfg, and EPOSesa.cfg files for the silent installation to work correctly.

  The Agent.settings file describes the SESA Agent settings. The MVSSesa.cfg file configures the Network Associates VirusScan Plug-in. The EPOSesa.cfg file configures the Network Associates ePolicy Orchestrator Plug-in. Depending on which Plug-in you are installing, you modify either the MVSSesa.cfg or EPOSesa.cfg file.

  See "Event Collector configuration file options" on page 49.

- Run the silent installation: Execute the Event Collector Installation Wizard with the proper command line to specify a silent installation of the Event Collector Framework and appropriate Plug-in.

To modify the necessary configuration files

1. On the computer on which you want to install the Event Collector, insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.
2. Copy the **\Collector** folder from the CD and paste it in a folder on the hard drive.
3. Change the privileges for the \Collector folder to write privileges.
4. At the command prompt, change directories to the \Collector folder on the hard drive.
5. In a text editor, open the **Agent.settings** file, then change or verify the following options:

mserverip	If SESA is using the default, anonymous SSL configuration, type the IP address of the SESA Manager to which the Event Collector will forward events. If SESA is using authenticated SSL, type the host name of the SESA Manager. For example, myserver.company.com.
mserverport	If necessary, type a new value for the port on which the SESA Manager listens. The default value is 443.

6. Save and close the **Agent.settings** file.

7 If you are installing the Network Associates VirusScan Plug-in, in a text editor, open the **MVSSesa.cfg** file, then change the values of the following options:

PluginLogPathCount	Type the number of log paths from which to forward logs. The default setting is 1. The number specified must match the number of log paths in the PluginLogPath*n* option or options. For example, if you have two PluginLogPath*n* entries, then the PluginLogPathCount value must equal 2.
PluginLogPath*n*	Type the full path of the VirusScan log. The default path is C:\Program Files\Network Associates\Virusscan. The number of PluginLogPath*n* entries must match the number value for the PluginLogPathCount option. You may type PluginLogPath lines, depending on how many VirusScan logs the Event Collector is reading. If a VirusScan log resides on a computer other than the one on which the Event Collector is installed, then the system account of the Symantec Collector Framework service must have read access rights to the computer on which the VirusScan log is stored. You can type UNC paths in the following format: \\server\share If no valid log path is specified, the associated Plug-in stops operating.
PluginForwardAllLogs	Type 1 to instruct the Event Collector installation program to forward, for one time only, all existing log data with new events. If set to 0 (off), this option instructs the Event Collector to forward only events that are generated after Event Collector installation. The default setting is 0.
PluginPollingFrequency	Type a number in seconds to check for new log records to process. The default setting is 5 seconds. The minimum time is 1 millisecond (0.001).

8 If you are installing the Network Associates ePolicy Orchestrator Plug-in, in a text editor, open the **EPOSesa.cfg** file, then verify or change the value of the following options:

PluginLogPathCount	Ensure that this option is set to 1. The ePO Policy Orchestrator Plug-in does not support multiple data sources. If multiple ePO databases exist, you must install one ePO Event Collector for each database.
PluginLogPath1	Type the full connection string to the ePO Database Server that the ePO Event Collector is using as a data source. The default ePO database connection string is: Provider=sqloledb;Data Source-<EPO_DATABASE_SERVER_NAME>;Initial Catalog=ePO_<EPO_SERVER_NAME>;Integrated Security=SSPI The default connection path specifies Windows Integrated Security, which authenticates to the ePO database under the user context of the Symantec Collector Framework service. If no valid log path is specified, the associated ePO Plug-in stops operating.
PluginForwardAllLogs	Type 1 to instruct the Event Collector installation program to forward, for one time only, all existing log data with new events. If set to 0 (off), this option instructs the Event Collector to forward only events that are generated after Event Collector installation. The default setting is 0.
PluginPollingFrequency	Type a number in seconds to check for new log records to process. The default setting is seconds. The minimum time is 1 millisecond (0.001).

9 Save and close the appropriate file.

To run the silent installation

1. On the computer on which you want to install the Event Collector, insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.
2. At the command prompt, change directories to the \Collector folder on the hard drive.
3. Type the following:

   setup.exe /s /v" /qn COLLECTOR=<Path> ADDLOCAL=Collector, <Plug-in name>"

   You type the following values:

<Path>	Local path and directory in which to install the Event Collector. The default location is C:\Program Files\Symantec\Collector. When you type a location that includes spaces, enclose the path in double quotes that are escaped with a backslash (\). For example: COLLECTOR=\"C:\Program Files\Symantec\Collector\"
<Plug-in name>	The ADDLOCAL property requires the Collector argument, but you must type one of the following Plug-in names, depending on the Network Associates Plug-in that you want to use: ■ MVSSesa (Network Associates VirusScan Plug-in) ■ EPOSesa (Network Associates ePolicy Orchestrator Plug-in)

The Symantec Collector Framework is added to the Add/Remove Programs dialog box, indicating that the Event Collector is installed. The SESA AgentStart Service and the Symantec Collector Framework service are added to the Windows Services window.

Changing the access rights of the Symantec Collector Framework service

If you plan to install the VirusScan Event Collector on a computer other than the one on which the VirusScan logs are installed, make sure that the Symantec Collector Framework service has at least read-only network access to the computer or computers on which the remote logs reside.

See "Suggested Event Collector installation configurations" on page 17.

If you plan to forward events from the Network Associates ePO database to SESA using Integrated Windows Authentication, you must ensure that the Symantec

Collector Framework service system account has at least query access to the ePO database.

Symantec Event Collector for Network Associates ePO and VirusScan installs the Event Collector as a service with local system access rights. You can change the access rights, or service credentials, of the Symantec Collector Framework service after the Event Collector is installed, if necessary.

To change the access rights of the Symantec Collector Framework service

1. On the computer on which the Event Collector is installed, in the Windows Services window, right-click **Symantec Collector Framework**, then click **Properties**.
2. In the Symantec Collector Framework Properties dialog box, on the Log On tab, click **This account**.
3. Type the user name and password of an account with the appropriate rights to access the source data that the Event Collector is using.
4. Click **OK** to save your changes and close the dialog box.

Adding other product Plug-ins to the Event Collector

You can modify the selection of Network Associates Plug-ins that are installed to the Event Collector. Symantec Event Collector for Network Associates ePO and VirusScan lets you add or remove Network Associates Plug-ins as necessary.

To add another product Plug-in to the Event Collector

1. On the computer on which the Event Collector is installed, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec Collector Framework**.
4. Click **Change**.
   The Installation Wizard starts.
5. In the Program Maintenance window, click **Modify**.
6. In the Custom Setup window, select the product Plug-in that you want to add.
7. Follow the on-screen instructions to install the Plug-in.

Configuring the ePO Event Collector for languages other than English

If you are using the ePO Event Collector and want it to collect VirusScan events in a language other than English, make sure that it is installed on a computer with an operating system in the same language.

Configure the Event Collector for languages other than English

To ensure correct character set translation, modify the language options in the following configuration files:

- EPOSesa.cfg: Specify the language ID of the language to use for VirusScan event descriptions and actions.
- Collector.cfg: Specify the language to use for events that are generated by the Event Collector Framework.

See "Language considerations" on page 20.

To configure the ePO Event Collector to collect VirusScan events in languages other than English

1. On the computer on which the ePO Event Collector is installed, navigate to the EPOSesa.cfg file.

   The default location is C:\Program Files\Symantec\Collector\Plugins\EPOSesa\Eposesa.cfg.
2. In a text editor, open **EPOSesa.cfg**.
3. For the EPOConnector_LanguageID option, type one of the following language IDs:
   - For French: 040C
   - For German: 0407
   - For Spanish: 040A
   - For English: 0409
   - For Japanese: 0411

   This option specifies the language in which VirusScan events are collected by the ePO Event Collector.
4. Save and close the **EPOSesa.cfg** file.

To configure the Event Collector Framework to generate events in languages other than English

1. On the computer on which the ePO Event Collector is installed, navigate to the Collector.cfg file.

   The default location is C:\Program Files\Symantec\Collector\Collector.cfg.
2. In a text editor, open **Collector.cfg**.
3. For the CollectorLocale option, type the language whose ID is specified in the EPOCollector_LanguageID option of the EPOSesa.cfg file.
4. Save and close the Collector.cfg file.

Verifying the installation

After installation, you can verify that the appropriate components are installed and working properly.

Verify the installation

To verify the installation, you do the following:

- Verify that the appropriate services have started.
- Verify that the Event Collector and Network Associates VirusScan are listed in the SESA Console.
- Examine the Event Collector and SESA Agent logs as necessary.

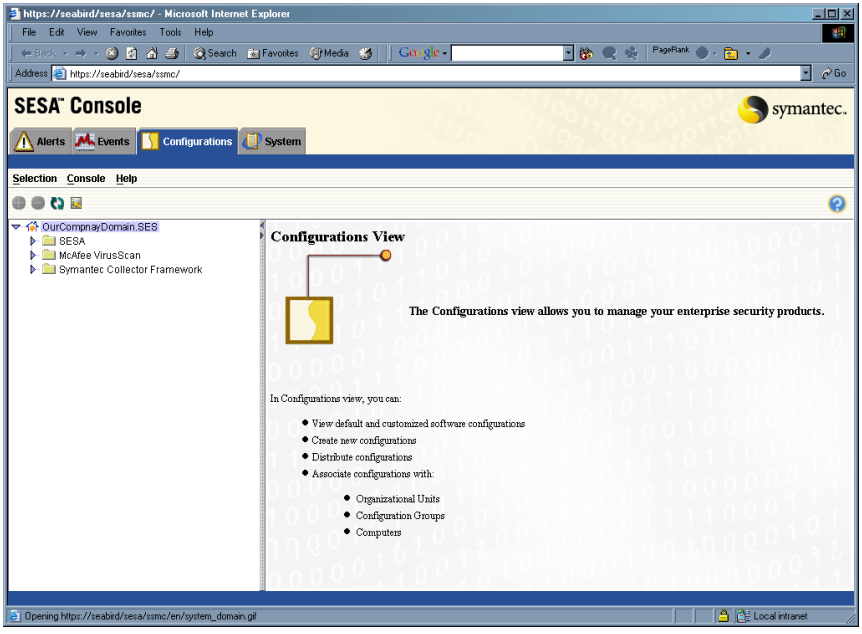
To verify that the appropriate services have started

- On the Event Collector computer, open the Services Control Panel and verify that the following services are installed:
  - SESA AgentStart Service
  - Symantec Collector Framework

To verify that the Event Collector and Network Associates VirusScan are displayed in the SESA Console

1. On the SESA Manager computer, on the Windows taskbar, click **Start** > **Programs** > **Symantec Enterprise Security**> **SESA Console**.
2. Log on to the SESA Console using a SESA user account with sufficient rights to view SESA configurations.

   The SESA user must belong to a Manager role that has rights to the SESA-enabled Symantec AntiVirus Corporate Edition product.
3. On the SESA Console, on the Events view tab, expand [**Top Level Domain.SES**] > **SESA DataStore** > **System Events**.
4. Under System Events, verify that the following items are listed:
   - Symantec Collector Framework
   - Network Associates VirusScan
5. Expand [**Top Level Domain.SES**] > **SESA DataStore** > **AntiVirus Event Family**.
6. Under AntiVirus Event Family, verify that Network Associates VirusScan is listed.
7. On the Configurations view tab, expand [**Top Level Domain.SES**].



8 Verify that the following items are listed:
   - Symantec Collector Framework
   - McAfee VirusScan

For more information on reports and views, see the *Symantec Enterprise Security Architecture Administrator's Guide.*

To examine the Event Collector and SESA Agent logs

1 On the computer on which the Event Collector is installed, navigate to the Collector log file, Collector.log.
   The default location is C:\Program Files\Symantec\Collector\Log\Collector.log.

2 Open and examine the log for the following entries:
   - The Symantec Collector Framework service was started.
   - The Symantec Collector plugin MVSSesa loaded successfully (if you installed the Network Associates VirusScan Plug-in).
   - The Symantec Collector plugin EPOSesa loaded successfully (if you installed the Network Associates ePolicy Orchestrator Plug-in).

3 Navigate to the SESA Agent log.
   The default location is C:\Program Files\Symantec\SESA\Agent\sesa-agent.log.

4 Ensure that the log contains the following entry:
   SESA Agent ***Bootstrap successful

Starting and stopping services

Symantec Event Collector for Network Associates ePO and VirusScan installs the following services on the computer on which the Event Collector is installed:

- Symantec Collector Framework
- SESA AgentStart Service

You can start and stop these Microsoft Windows services as necessary.

To start or stop a service

1. On the computer on which you installed the Event Collector, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Administrative Tools**.
3. In the Administrative Tools window, double-click **Services**.
4. In the Services dialog box, right-click the service that you want to start or stop, then click **Start** or **Stop**.

Note: When you make a change to the MVSSesa.cfg or EPOSesa.cfg file, you must restart the Symantec Collector Framework service for the changes to take effect.

As an alternative, you can use Event Collector command-line options to load and unload (start and stop) Plug-ins. This way, you can modify the MVSSesa.cfg and EPOSesa.cfg files without having to restart the Symantec Collector Framework service.

See "Event Collector command-line options" on page 62.

Troubleshooting the Symantec Event Collector for Network Associates ePO and VirusScan installation

If you are not receiving Network Associates VirusScan events after Symantec Event Collector for Network Associates ePO and VirusScan installation, performing the following procedures allows you to confirm operation:

- Verifying SESA integration component installation
- Verifying Event Collector operation
- Troubleshooting the Network Associates ePolicy Orchestrator Plug-in
- Troubleshooting the Network Associates VirusScan Plug-in

Verifying SESA integration component installation

Verify that you specified the correct SESA Manager IP address (or host name) and the correct number for the SESA secure Directory port when you ran the SESA Integration Wizards.

To verify the correct SESA integration component information

1. On the Event Collector computer, at the command prompt, change directories to the \Collector folder on the hard drive.
2. In a text editor, open the **Agent.settings** file.
3. Verify that the following options are set correctly:
   - mserverip
   - mserverport

Verifying Event Collector operation

You can verify Event Collector operation by confirming that the proper services are running.

To verify Event Collector operation

1. On the Event Collector computer, open the Services Control Panel and verify that the following services are running:
   - Symantec Collector Framework service
   - SESA AgentStart Service
2. Open the Windows Event Viewer and examine the Application Log for any of the following failure events from the (Event) Collector:

Plugin <name> Failed to load.	Typically, a mismatch in the Plug-in file and configuration paths exists. To check for mismatched paths, continue with the next step.
The LogPath <path> is invalid.	The configured path to the VirusScan log files does not exist, or the Event Collector does not have sufficient access rights to access the local or remote folders.
The data source <connection string> is invalid.	The specified ePO database connection string is incorrect or the Symantec Collector Framework service does not have sufficient access rights to read the ePO database.

If you see only success events, the problem probably exists elsewhere.

3. At the command prompt, change directories to the Symantec Event Collector for Network Associates ePO and VirusScan installation folder.

   The default location is C:\Program Files\Symantec\Collector.

4. Type the following:

   collector.exe -plugininfo

   The Event Collector displays Plug-in information on the screen.

5. Verify the following:

   - The appropriate Plug-in exists and its Load parameter setting is 1.
   - The Plug-in file (DLL) path and the Plug-in configuration file paths contain the files specified.

Troubleshooting the Network Associates ePolicy Orchestrator Plug-in

If you have installed the Network Associates ePolicy Orchestrator Plug-in, first verify that the ePO database is successfully receiving Network Associates VirusScan event data.

If the ePO database is not receiving event data, then a problem exists between the ePolicy Orchestrator Server and client computers. See your Network Associates ePolicy Orchestrator documentation for troubleshooting information.

If the ePO database is receiving Network Associates VirusScan event data, verify that the ePolicy Orchestrator Plug-in configuration file (EPOSesa.cfg) is correctly configured to process events.

To verify that EPOSesa.cfg is correctly configured to process events

1. On the computer on which the ePO Event Collector is installed, navigate to the EPOSesa.cfg file.

   The default location is C:\Program Files\Symantec\Collector\Plugins\EPOSesa\Eposesa.cfg.

2. In a text editor, open **EPOSesa.cfg**.

3. Verify that the EPOConnector_LastHandledEvent option is set to greater than zero (>0). If the setting is less than zero, then the Plug-in is unable to successfully process VirusScan events.

If the Plug-in is successfully processing events, then the problem is probably caused by the SESA Agent or the SESA Manager.

See "Verifying SESA integration component installation" on page 41.

See "Verifying Event Collector operation" on page 42.

Troubleshooting the Network Associates VirusScan Plug-in

If you have installed the Network Associates VirusScan Plug-in, verify that the Network Associates VirusScan Plug-in configuration file (MVSSesa.cfg) exists and is configured correctly.

To verify that MVSSesa.cfg exists and is configured correctly

1. On the computer on which the VirusScan Event Collector is installed, navigate to the MVSSesa.cfg file.

   The default location is C:\Documents and Settings\All Users\Application Data\Symantec\Collector\Plugins\MVSSesa.

2. Examine the MVSSesa folder for MVSSesa*n*.sts files.

   The *n* is the index of the VirusScan log path that you are troubleshooting.

   If the file does not exist, then the VirusScan Plug-in is unable to retrieve and process events.

   If the file does exist and it contains file names followed by a number, then the VirusScan Plug-in is successfully processing events, and the problem is probably with the SESA Agent or the SESA Manager.

   See "Verifying SESA integration component installation" on page 41.
   See "Verifying Event Collector operation" on page 42.

Uninstalling Symantec Event Collector for Network Associates ePO and VirusScan

You uninstall Symantec Event Collector for Network Associates by completing the following tasks:

- Uninstall the Event Collector and SESA Agent.
- Uninstall the SESA integration components for the Event Collector Framework and Network Associates VirusScan as necessary.

Uninstalling the Event Collector

You can uninstall the Event Collector and SESA Agent using the Microsoft Windows Add/Remove Programs feature or by executing a command at the command prompt.

When you remove the Event Collector, the uninstallation program removes the Event Collector Framework, the installed Network Associates Plug-ins, and the SESA Agent.

Uninstall the Event Collector

You can uninstall the Event Collector by using the Microsoft Windows Add/Remove Programs feature. You can also uninstall the Event Collector by command line if you want to avoid displaying Add/Remove Programs windows. This type of command-line uninstallation is called a silent uninstall.

You can perform a silent uninstall from any directory (with or without the installation media), or you can perform a silent uninstall from the installation media location.

To uninstall the Event Collector using Add/Remove Programs

1. On the computer on which the Event Collector is installed, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Add/Remove Programs**.
3. In the Add/Remove Programs dialog box, click **Symantec Event Collector for Network Associates ePO and VirusScan**, then click **Remove**.
4. When you are prompted to remove Symantec Event Collector for Network Associates ePO and VirusScan from your computer, click **Yes**.

Symantec Event Collector for Network Associates ePO and VirusScan is removed from the Add/Remove Programs dialog box, indicating that the Event Collector is removed. The SESAAgentStart service and the Symantec Collector Framework service are removed from the Windows Services window (service control manager).

To perform a silent uninstall from any directory

- On the computer on which the Event Collector is installed, at the command prompt, type the following:
  msiexec /x {1EFA0190-DF57-4884-BD07-4E71D08990A2} /qn

To perform a silent uninstall from the installation media directory

1. On the computer on which the Event Collector is installed, do one of the following:
   - Insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive, then change directories on the CD to the \Collector folder.
   - Change to the \Collector directory on the computer.
2. At the command prompt, type the following:
   msiexec /x "Setup.msi" /qn

Symantec Event Collector for Network Associates ePO and VirusScan is removed from the Add/Remove Programs window, indicating that the Event Collector is removed. The SESAAgentStart service and the Symantec Collector Framework service are removed from the Windows Services window (service control manager).

Uninstalling the SESA integration components

To uninstall the SESA integration components for Network Associates VirusScan, you must run the SESA Integration Wizard for the Event Collector Framework and again for the Network Associates VirusScan Plug-in.

Uninstall the SESA integration components

To remove the SESA integration components for Network Associates VirusScan, run the SESA Integration Wizard for the following:

- Event Collector Framework
- Network Associates VirusScan

To uninstall Event Collector Framework integration components from SESA

1. On the SESA Manager computer, insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.
2. At the command prompt, change directories on the CD to Collector\SESA.
3. Type the following command to launch the SESA Integration Wizard:
   java –jar setup.jar –uninstall
4. Follow the on-screen instructions until you see the SESA Domain Administrator Information window.

5 In the SESA Domain Administrator Information window, provide the following information that was used when SESA was originally installed:

SESA Domain Administrator Name	Type the SESA Domain Administrator account name. This account was created during SESA installation or after installation from within SESA.
SESA Domain Administrator Password	Type the administrator password.
Host Name or IP Address of SESA Directory	Type one of the following: ■ IP address of the SESA Directory: Use the IP address if SESA is installed with the default, anonymous, self-signed SSL certificate. ■ Hostname of the SESA Directory: Use the hostname if SESA is upgraded to use an authenticated, self-signed SSL certificate or Certificate Authority-signed SSL certificate.
Secure Directory Port	Type the number of the SESA Directory SSL (LDAP) port (by default, 636).

The SESA Integration Wizard removes the SESA integration components for the Event Collector Framework.

To complete the uninstallation for Symantec Event Collector for Network Associates ePO and VirusScan, uninstall the SESA integration components for Network Associates VirusScan.

See "To uninstall Network Associates VirusScan integration components from SESA" on page 47.

To uninstall Network Associates VirusScan integration components from SESA

1 On the SESA Manager computer, insert the Symantec Event Collector for Network Associates ePO and VirusScan CD into the CD-ROM drive.

2 At the command prompt, change directories on the CD to VirusScan\SESA.

3 Type the following command to launch the SESA Integration Wizard:
java –jar setup.jar –uninstall

4 Follow the on-screen instructions until you see the SESA Domain Administrator Information window.

5 In the SESA Domain Administrator Information window, provide the following information that was used when SESA was originally installed:

SESA Domain Administrator Name	Type the SESA Domain Administrator account name. This account was created during SESA installation or after installation from within SESA.
SESA Domain Administrator Password	Type the administrator password.
Host Name or IP Address of SESA Directory	Type one of the following: ■ IP address of the SESA Directory: Use the IP address if SESA is installed with the default, anonymous, self-signed SSL certificate. ■ Hostname of the SESA Directory: Use the hostname if SESA is upgraded to use an authenticated, self-signed SSL certificate or Certificate Authority-signed SSL certificate.
Secure Directory Port	Type the number of the SESA Directory SSL (LDAP) port (by default, 636).

The SESA Integration Wizard removes the SESA integration components for Network Associates VirusScan.

Appendix A

Event Collector configuration file options

This chapter includes the following topics:

- Collector.cfg file configuration options
- MVSSesa.cfg file configuration options
- EPOSesa.cfg file configuration options

Collector.cfg file configuration options

Collector.cfg contains the configurations that manage the Event Collector Framework.

Table A-1 lists the options that you can configure for the Collector.cfg file.

Table A-1 Collector.cfg file configuration options

Option	Description
CollectorLocale	Specifies the language locale that produced the logs (for example, CollectorLocale=Japanese). You must specify the operating system language of the computer on which the Event Collector is installed.
ConfigPollInterval	Specifies, in seconds, how often to query Collector.cfg for changes. This option is monitored for real-time updates. The default setting is 15 seconds.
SystemEventLog	Enables or disables logging to the Windows NT event log. The default setting is 1 (on). A setting of 0 disables logging. If the LogFile and LogSESA options are also enabled, the same information is logged to the Event Collector log and SESA DataStore.
LogFile	Specifies the path of the text log file for the Event Collector. A full path is required. The default path is C:\Collector\log.txt. If the SystemEventLog and LogSESA options are also enabled, the same information is logged to the Windows NT event log and SESA DataStore.
LogSESA	Enables or disables logging to the SESA DataStore. The default setting is 1 (on). A setting of 0 disables logging to the SESA DataStore. If the SystemEventLog and LogFile options are also enabled, the same information is logged to the Windows NT event log and Event Collector log.
PluginCount	Indicates the number of product Plug-ins that have been installed to the Event Collector Framework. The number that you specify for PluginCount must match the number of Plugin*n* entries contained in the Collector.cfg file.

Table A-1 Collector.cfg file configuration options

Option	Description
Plugin*n*	Specifies the name of the product Plug-in. This option is set during installation. Each Plug-in has a separate Plugin*n* line. The number of Plugin*n* entries must match the number specified for PluginCount.
<Plug-in name>_File	Specifies the full path name of the <Plug-in name> DLL file. This is set during installation.
<Plug-in name>_Config	Specifies the full path of the <Plug-in name> configuration file. This is set during installation.
<Plug-in name>_Load	Specifies whether the installed Plug-in has been started. The default setting is 1. A setting of 0 indicates that the Plug-in has not been started. This is set during installation.

MVSSesa.cfg file configuration options

MVSSesa.cfg contains the configurations that manage the Network Associates VirusScan Plug-in.

Table A-2 lists the options that you can configure for the MVSSesa.cfg file.

Table A-2 MVSSesa.cfg file configuration options

Option	Description
PluginLocale	Specifies the language locale that produced the logs (for example: PluginLocale = Japanese). You must specify the operating system language of the computer on which the Event Collector is installed.
PluginPollingFrequency	Specifies how often, in seconds, to check for new log records to process. The default setting is 5 seconds. The minimum time is 1 millisecond (0.001).
PluginBurstCount	Specifies the number of log records to process during each polling cycle. The polling frequency is set by PluginPollingFrequency. The default setting is 25.

Table A-2 MVSSesa.cfg file configuration options

Option	Description
PluginForwardAllLogs	If set to 1 (on), instructs the Event Collector installation program to forward, for one time only, all existing log data with new events. If set to 0 (off), instructs the Event Collector to forward only events that are generated after Event Collector installation. The default setting is 0.
PluginLogPathCount	Specifies the number of log paths from which to forward logs. The default setting is 1. The number specified must match the number of log paths in the PluginLogPath*n* option or options. For example, if you modify the MVSSesa.cfg file to include two PluginLogPath*n* entries, then the PluginLogPathCount value must equal two.
PluginDebugLevel	If set to 1 (on), sends additional information to the Event Collector log, SESA, or the Windows NT event log. The default setting is 0 (off).
PluginLogPath*n*	Specifies the full path of the VirusScan log. You can type UNC paths in the following format: \\server\share There may be multiple PluginLogPath lines, depending on how many VirusScan logs that the Event Collector is reading. If a VirusScan log resides on a computer other than the one on which the Event Collector is installed, then the system account of the Symantec Collector Framework service must have read access rights to the computer on which the VirusScan log is stored. The number of PluginLogPath*n* entries must match the number value for the PluginLogPathCount option. If no valid log path is specified, the associated Plug-in stops operating.

EPOSesa.cfg file configuration options

EPOSesa.cfg contains the configurations that manage the Network Associates ePolicy Orchestrator Plug-in.

Table A-3 lists the options that you can configure for the EPOSesa.cfg file.

Table A-3 EPOSesa.cfg file configuration options

Option	Description
PluginPollingFrequency	Specifies how often, in seconds, to check for new log records to process. The default setting is 5 seconds. The minimum time is 1 millisecond (0.001).
PluginBurstCount	Specifies the number of log records to process during each polling cycle. The polling frequency is set by PluginPollingFrequency. The default setting is 25.
PluginForwardAllLogs	If set to 1 (on), instructs the Event Collector installation program to forward, for one time only, all existing log data with new events. If set to 0 (off), instructs the Event Collector to forward only events that are generated after Event Collector installation. The default setting is 1.
PluginLogPathCount	Specifies how many databases to monitor. This value must be set to 1. The ePO Policy Orchestrator Plug-in does not support multiple data sources. If multiple ePO databases exist, you must install one ePO Event Collector for each database.
PluginDebugLevel	If set to 1 (on), sends additional information to the Event Collector log, SESA, or the Windows NT event log. The default setting is 0 (off).

Table A-3 EPOSesa.cfg file configuration options

Option	Description
PluginLogPath1	Specifies the full connection string to the ePO Database Server that the ePO Event Collector is using as a data source. The default ePO database connection string is: Provider=sqloledb;Data Source=<EPO_DATABASE_SERVER_NAME>; InitialCatalog=ePO_<EPO_SERVER_NAME>; Integrated Security=SSPI The default connection path specifies Windows Integrated Security, which authenticates to the ePO database under the user context of the Symantec Collector Framework service. If no valid log path is specified, the associated ePO Plug-in stops operating.
EPOConnector_LastHandledEvent	Specifies the ID of the last handled event from the ePO database. This is automatically incremented as the ePolicy Orchestrator Plug-in processes events. To begin processing from the first event in the ePO database, set this option to 0.
EPOConnector_LanguageID	Specifies the language identifier (ID) for ePolicy Orchestrator. VirusScan event descriptions are retrieved from the ePO database in the language that this option specifies. You can specify the following language IDs: ■ 040C (French) ■ 0407 (German) ■ 040A (Spanish) ■ 0409 (English) ■ 0411 (Japanese)

Appendix B

Command-line options

This chapter includes the following topics:

- Installing Symantec Event Collector for Network Associates ePO and VirusScan components manually
- Installing the SESA Agent
- Guidelines for using scripts to install the Event Collector
- Event Collector command-line options
- SESA Integration Wizard command-line options

Installing Symantec Event Collector for Network Associates ePO and VirusScan components manually

You may want to install or uninstall individual components of the Symantec Event Collector for Network Associates ePO and VirusScan. You can do so by using the command-line options that the Event Collector provides.

If you are installing the Event Collector by command line, you must first install the SESA Agent manually. To install all of the components of Symantec Event Collector for Network Associates ePO and VirusScan, complete the following tasks in the order in which they are listed:

- Install the SESA Agent for Symantec Event Collector for Network Associates ePO and VirusScan.
- Install the Event Collector by command line.
- Install the required Plug-in by command line.
- Start the Plug-ins by command line.

To uninstall Symantec Event Collector for Network Associates ePO and VirusScan, you complete the tasks in reverse order using the appropriate uninstall command-line options.

Installing the SESA Agent

To install the SESA Agent separately by command line, you must access the SESA Agent files on the Symantec Enterprise Security Architecture CD1 - SESA Manager.

The computer on which you install the SESA Agent must be running Java Runtime Environment (JRE) versions 1.2.2_008 through 1.3.1_02 or be hosting the SESA Manager.

Install the SESA Agent

To install the SESA Agent, you do the following:

- Install JRE on the target computer, if necessary.
- Prepare to install the SESA Agent.
- Install the SESA Agent by command line.

Note: When you install the SESA Agent manually by command line, you must also uninstall it manually by command line.

To install JRE on the target computer

1. On the SESA CD1 - SESA Manager, in the \Utils\JRE folder, double-click **j2re-1_3_1_02-win-i.exe**.
2. Follow the on-screen instructions.

To prepare to install the SESA Agent

1. On the computer on which you want to install the SESA Agent (and the Event Collector), insert the SESA CD1 - SESA Manager into the CD-ROM drive.
2. Copy the **\Agent\agent.settings** file from the CD and paste it in a Temp folder on the hard drive.
3. In a text editor, open the **Agent.settings** file.
4. Change the value of the mserverip setting to the IP address of the SESA Manager to which the Event Collector will forward events.
5. Save and close the **Agent.settings** file.

To install the SESA Agent by command line

1. On the computer on which you want to install the Event Collector, at the command prompt, change directories to \Agent.
2. At the command prompt, type the following:

   java -jar agentinst.jar -a<ProdID> -f<Filename>

   <Filename> is the full path of the Agent.settings file that you copied to the Temp folder on the Event Collector computer. If the Filename path contains spaces, you must enclose the path in double quotation marks.

   The argument <ProdID> is a unique ID for the product for which you want to install the SESA Agent. You can use any combination of single-byte characters as long as you uninstall the SESA Agent using the same product ID (ProdID).

   For example, for Network Associates VirusScan, you can specify -aNETAVS.

   Optionally, you can append any of the following parameters:

-debug	Writes logging information to the screen
-log	Turns off the installation log and instructs the SESA Agent to write logging information to the Agntinst.log file in the local Temp directory

Uninstalling the SESA Agent

When you remove a SESA Agent, you must use the same product ID (ProdID) that you used to install it.

See "Installing the SESA Agent" on page 56.

Uninstall the SESA Agent

To remove the SESA Agent, you do the following:

- Stop the SESA AgentStart Service.
- Remove the SESA Agent.

Note: You must uninstall the SESA Agent using the same product ID (ProdID) command-line parameter that you used to install it.

To stop the SESA AgentStart Service

1 On the computer on which you installed the Event Collector, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.

2 In the Control Panel window, double-click **Administrative Tools**.

3 In the Administrative Tools window, double-click **Services**.

4 In the Services dialog box, right-click the **SESA AgentStart Service**, then click **Stop**.

To uninstall the SESA Agent manually

1 On the computer on which you want to install the Event Collector, at the command prompt, change directories to \Agent.

2 At the command prompt, type the following:

java -jar agentinst.jar -u -a<ProdID>

The argument <ProdID> is a unique ID for the product for which you want to uninstall the SESA Agent. You must use the product ID (ProdID) that you used to install the SESA Agent.

Optionally, you can append any of the following parameters:

-debug	Writes logging information to the screen
-log	Turns off the installation log and instructs the SESA Agent to write logging information to the Agntinst.log file in the local Temp directory

Guidelines for using scripts to install the Event Collector

You may want to install or uninstall the Event Collector Framework and the Network Associates ePolicy Orchestrator or VirusScan Plug-in by using scripts and distributing them with Event Collector files as necessary.

You can include Event Collector command-line options in scripts to do the following:

- Install and uninstall the Event Collector Framework.
- Install and uninstall the Network Associates Plug-ins.
- Load and unload the Network Associates Plug-ins (start and stop the Plug-ins).

See Table B-1, "Event Collector command-line options," on page 63.

To install the Event Collector using a script, you must have access to the following Event Collector files:

- Collector.exe
- Collres.dll
- Collutil.dll
- Collector.cfg

You can obtain the files from your existing installation of the Event Collector.

Depending on how many SESA-enabled products are using the SESA Agent on a given Event Collector computer, you may also want to include scripts for installing or uninstalling the SESA Agent.

See "Uninstalling the SESA Agent" on page 58.

To install (or uninstall) Symantec Event Collector for Network Associates ePO and VirusScan completely, you must also install (or uninstall) the SESA integration components for your product. You can install or uninstall these components by using SESA Integration Wizard command-line options.

See "SESA Integration Wizard command-line options" on page 64.

Event Collector installation scripts

To install the Event Collector Framework and Network Associates Plug-ins, use the following Event Collector command-line options (in shortcut syntax) in your installation script:

collector -install	Registers the Event Collector Framework with the Windows service control manager and the Windows NT event log as the Symantec Collector Framework service
collector -pa:<Name> -pf:<Filename1> -pc:<Filename2>	Installs the Plug-in without loading it
collector -pl:<Name>	Loads the Plug-in

See "Event Collector command-line options" on page 62.

Event Collector uninstallation scripts

To uninstall the Event Collector Framework and Network Associates Plug-ins, use the following Event Collector command-line options (in shortcut syntax) in your uninstall script:

collector -pu:<Name>	Unloads the Plug-in
collector -pr:<Name>	Uninstalls the Plug-in
collector -uninstall	Unregisters the Event Collector Framework (Symantec Collector Framework service) from the Windows service control manager and the Windows NT event log

See "Event Collector command-line options" on page 62.

Deleting Event Collector and SESA Agent files

When you use Event Collector command-line options to uninstall Event Collector components, you must also delete the Event Collector and SESA Agent files from the Event Collector computers, if desired.

To delete the Event Collector and SESA Agent files

- On the computer on which you want to remove the Event Collector, delete the following folders as necessary:
  - \Collector
  - \Agent

  The default location for Event Collector files is C:\Program Files\Symantec\Collector. The default location for SESA Agent files is C:\Program Files\Symantec\SESA\Agent.

Plug-in installation and uninstallation scripts

To install or uninstall the Network Associates Plug-ins only, use the following Event Collector command-line options (in shortcut syntax) in your script, as appropriate:

collector -pa:<Name> -pf:<Filename1> -pc:<Filename2>	Installs the Plug-in without loading it
collector -pl:<Name>	Loads the Plug-in
collector -pu:<Name>	Unloads the Plug-in
collector -pr:<Name>	Uninstalls the Plug-in

See "Event Collector command-line options" on page 62.

Plug-in load and unload scripts

To load or unload Network Associates Plug-ins, use the following Event Collector command-line options (in shortcut syntax) in your script, as appropriate:

collector -pl:<Name>	Loads the Plug-in
collector -pu:<Name>	Unloads the Plug-in

See "Event Collector command-line options" on page 62.

Event Collector command-line options

Table B-1 contains the command-line options that are available in the Event Collector. Event Collector command-line options must have access to a number of installed Event Collector files, and are therefore not typically available until after the Event Collector is initially installed. To use a command-line option with a Network Associates Plug-in, that Plug-in must have been installed; otherwise, the post-installation Plug-in files on which the command-line options rely will not be available.

See "Guidelines for using scripts to install the Event Collector" on page 59.

See "Installing Symantec Event Collector for Network Associates ePO and VirusScan" on page 23.

See "Installing the Event Collector silently" on page 31.

When you execute a command-line option, configuration changes are made to the Collector.cfg file.

Table B-1 Event Collector command-line options

Command-line option	Description
-install	Installs the Event Collector Framework.
-uninstall	Unregisters the Event Collector Framework from the Windows service control manager and Windows NT event log.
-pluginadd:<Name> -pluginfile:<Filename1> -pluginconfig:<Filename2> Shortcut: -pa:<Name> -pf:<Filename1> -pc:<Filename2>	Adds the specified Plug-in to the Event Collector Framework. You must specify all options. <Name> is the name of the Plug-in to add as specified in the Plugin*n* option of the Collector.cfg file. For example, MVSSesa. Plug-in names are case-sensitive. <Filename1> is the name of the Plug-in DLL file. For example, "C:\Program Files\Symantec\Collector\Plugins\MVSSesa\mvssesa.dll" <Filename2> is the name of the Plug-in configuration file. For example, "C:\Program Files\Symantec\Collector\Plugins\MVSSesa\mvssesa.cfg" Any paths that contain spaces must be enclosed in double quotation marks.
-pluginload:<Name> [-wait:<0:1>] Shortcut: -pl:<Name>[-w:<0 |1>]	Starts the specified Plug-in. <Name> is the name of the Plug-in to add as specified in the Plugin*n* option of the Collector.cfg file. For example, MVSSesa. Plug-in names are case-sensitive. To have the Event Collector program wait until the Plug-in has started before returning control to you, append the following argument: -wait:1 To have the Event Collector program return control to you instantly, append the following argument: -wait:0 The default is 0 (wait disabled).
-pluginremove:<Name> Shortcut: -pr:<Name>	Uninstalls the specified Plug-in from the Event Collector Framework. <Name> is the name of the Plug-in to add as specified in the Plugin*n* option of the Collector.cfg file. For example, MVSSesa. Plug-in names are case-sensitive.

Table B-1 Event Collector command-line options

Command-line option	Description
-pluginunload:<Name> [-wait:<0:1>]	Stops the Symantec Collector Framework service.
Shortcut: -pu:<Name> [-w:<0 |1>]	<Name> is the name of the Plug-in to add, as specified in the Plugin*n* option of the Collector.cfg file. For example, MVSSesa. Plug-in names are case-sensitive. To have the Event Collector program wait until the Plug-in has started before returning control to you, append the following argument: -wait:1 To have the Event Collector program return control to you instantly, append the following argument: -wait:0 The default is 0 (wait disabled).
-h	Displays the available Event Collector command-line options.
-plugininfo[:<Name>]	Displays the status and associated DLL and configuration files for all Plug-ins or the specified Plug-in. For example, Collector -status:MVSSesa Plug-in names are case-sensitive.

SESA Integration Wizard command-line options

The SESA Integration Wizard provides command-line options that you can use in place of the SESA Integration Wizard.

The SESA Integration Wizard command to use with the command-line options is the following:

java -jar setup.jar

For example, to install the SESA integration components without displaying the SESA Integration Wizard, you would append the command-line option for a silent installation as follows:

java -jar setup.jar -silent -userDN<userdn> -password <password> -sesaDirectory<hostname> -sesaDirectoryPort<port>

Table B-2 contains the command-line options that you can use instead of the SESA Integration Wizard to install SESA integration components.

Table B-2 SESA Integration Wizard command-line options

Command-line option	Description
-debug	Prints debug information and creates a SIPIInst.log in the Temp folder (C:\Documents and Settings\USERNAME\Local Settings\Temp) with all of the debug information.
-silent	Runs the SESA Integration Wizard without displaying screens. You must also append the following command-line options: ■ -userDN <userdn> ■ -password <password> ■ -sesaDirectory <hostname> ■ -sesaDirectoryPort <port>
-userDN <userdn>	Specifies the user name that is used to connect to the SESA Directory (required for a silent installation).
-password <password>	Specifies the password that is used to connect to the SESA Directory (required for a silent installation).
-sesaDirectory <hostname>	Specifies the computer host name or IP address of the SESA Directory (required for a silent installation).
-sesaDirectoryPort <port>	Specifies the port number of the SESA Directory (required for a silent installation).
-info	Displays information about the SESA Integration Wizard installation, including the product and version information.
-help	Displays all available arguments.
-uninstall	Uninstalls the schema that is installed by integrated products from the SESA Directory and SESA DataStore. All events that were logged by the product are also deleted.

Index

A

access rights, Event Collector and Network Associates VirusScan logs or ePO database 33, 35, 36, 52
Add/Remove Programs, Event Collector 45
Agent.settings file 40, 57
authentication
    See also Secure Sockets Layer
    SQL Server 31

B

before installation. *See* pre-installation
bootstrap, SESA Agent 40

C

CD contents, Symantec Event Collector for Network Associates ePO and VirusScan 13
Collector.cfg file 50
CollectorLocal configuration option 50
command-line options
    Event Collector 62
    SESA Integration Wizard 56, 64
    uninstalling
        Event Collector Framework 61
        Plug-ins 61
component installation, individual 56
configuration options
    Agent.settings file 40, 57
    CollectorLocale 50
    Event Collector 50
    mserverip 32, 42, 57
    mserverport 32, 42
    Network Associates ePolicy Orchestrator (ePO) Plug-in 53
    Network Associates VirusScan Plug-in 51
    operating systems in languages other than English 37
    PluginLocale 51
    PluginLogPathCount 20, 52, 53
configuration options *(continued)*
    PluginLogPath*n* 20, 52, 54

E

EPOSesa.cfg file 53
Event Collector
    access rights to VirusScan logs or ePO database 33, 35, 36, 52
    Add/Remove Programs 45
    adding Plug-ins 36
    Collector.cfg file 50
    command-line options 56, 62
    configuring for languages other than English 37
    installing
        silently 31
        using Event Collector Installation Wizard 27
    log, examining 40
    scripting guidelines 59
        Event Collector install command-line option 60
        Event Collector uninstall command-line option 61
        Plug-in command-line options 62
    setup, planning 16
    suggested installation configurations 17
    system requirements 22
    uninstalling, using Add/Remove Programs 44
Event Collector Framework
    service
        starting and stopping 40
        startup verification 38
    uninstalling
        by Event Collector command-line option 61

G

guidelines, scripting 59

I

installation
Event Collector
silent 35
using Installation Wizard 28
using scripting 59
JRE (Java Runtime Environment) 57
manually by component 56
phases 23
suggested Event Collector configurations 17
Symantec Event Collector for Network Associates ePO and VirusScan, verifying 38
troubleshooting 41

J

Japanese language 21
JRE (Java Runtime Environment), installing 16, 57

L

language locale 50, 51
logs
Event Collector 40
Event Collector polling frequency 30
Network Associates VirusScan 17, 19, 30
SESA Agent 40
Windows NT event 50, 63

M

McAfee. *See* Network Associates
mserverip setting 32, 42, 57
mserverport setting 32, 42
MVSSesa.cfg file 41, 51

N

network access, Event Collector and Network Associates VirusScan logs or ePO database 33, 35, 36, 52
Network Associates ePolicy Orchestrator (ePO)
database
Event Collector access rights 36
SQL Server authentication 31
Windows integrated authentication 31
Network Associates ePolicy Orchestrator (ePO) *(continued)*
Plug-in
command-line options 63
configuration options 53
when to install 24
supported versions 22
Network Associates VirusScan 30
logs
Event Collector access rights 36
Event Collector polling frequency 17, 51
MVSSesa.cfg file 41
Plug-in
command-line options 63
configuration options 51
when to install 24
supported versions 22

O

operating systems
configuration options for languages other than English 50, 51
in languages other than English 37, 38
system requirements 22

P

Phases of installation 23
PluginLocale option 51
PluginLogPathCount option 20, 52, 53
PluginLogPath*n* option 20, 52, 54
Plug-ins
adding 36
Network Associates ePolicy Orchestrator Plug-in configuration file 53
Network Associates VirusScan Plug-in configuration file 51
uninstalling by command-line option 61
pre-installation, Symantec Event Collector for Network Associates ePO and VirusScan 16
product
ID for Network Associates VirusScan 58, 59
Plug-ins. *See* Plug-ins
products supported 10

R

removing. *See* uninstalling
RunAsService 23, 28

S

scripting, guidelines 59
Secure Sockets Layer (SSL) 26, 27, 29, 47, 48
services, starting and stopping 40
SESA
  about 11
  integration components
    installing 25
    uninstalling 46
  operation, verifying 42
SESA Agent
  installing manually 56
  log, examining 40
  preparing to install 57
  startup verification 38
  system requirements. *See* Event Collector, system requirements
  uninstalling 58
SESA AgentStart Service, starting and stopping 40
SESA Console
  logging onto 39
  Network Associates VirusScan, viewing 39
  operation 10
SESA Integration Wizard
  about 24
  command-line options 64
  Event Collector Framework 25
  Network Associates VirusScan or ePolicy Orchestrator 26
silent installation, Event Collector 31
SQL Server authentication 31
suggested Event Collector installation configurations 17
supported products 10
Symantec Collector Framework service
  addition to Windows service control manager 35
  changing access rights 36
  entries in SESA Agent log 40
  stopping and starting 41
Symantec Event Collector for Network Associates ePO and VirusScan
  about 11, 24
  CD contents 13
  Event Collector command-line options 56
  installing
    Event Collector 27
    SESA integration components 25
  SESA Integration Wizard command-line options 65
  system requirements for SESA integration 22
  uninstalling 44
  using with your product 11
system requirements
  Symantec Event Collector for Network Associates ePO and VirusScan 22

T

troubleshooting installation 41

U

uninstalling
  Event Collector 44
  SESA integration components
    Event Collector Framework 46
    Network Associates VirusScan 47

V

verification
  of integration with Symantec Event Collector for Network Associates ePO and VirusScan 38
  of SESA operation 42

W

Windows NT event log 50, 63